CORRIGENDUM TO

REQUEST FOR PROPOSAL

RFP Reference - NTB/IT/INFRA/2018/12/002

SUPPLY, INSTALLATION, TESTING AND COMMISSIONING (SITC) OF ICT INFRASTRUCTURE AT DC, NEAR DR AND FAR DR HOSTED AT SERVICE PROVIDER DATA CENTER AND MANAGED TELECOM AT ALL THE NAINITAL BANK LIMITED BRANCHES/OFFICES WITH OPERATION & MAINTENANCE

The Nainital Bank Limited
11th Jan 2019
RFP Reference - NTB/IT/INFRA/2018/12/002

3.30 Evaluation of Eligibility Criteria

ELIGIBILITY CRITERIA		
Sr. No.	**Specification as per original RFP Document**	**Amendment**
2	The bidder's average annual turnover should be at least INR. 300 Crores from Indian operations in each of last three financial years. The bidder's annual turnover from Data Centre Services and Cloud & Managed Services should be at least (INR) 100 crores in each of the last three financial years in India. The bidder should be a profit making entity over the past 3 years in India	The bidder's average annual turnover should be at least INR. 200 Crores from Indian operations in each of last three financial years. The bidder's annual turnover from Data Centre Services and Cloud & Managed Services should be at least (INR) 100 crores in each of the last three financial years in India. The bidder should be a profit making entity over the past 3 years in India.
3	Infrastructure at the Data Center should be in compliance to industry renowned standards, highlighted below) TIA 942 standard (Telecommunications Industry Association standard for Building, Network Design & Cabling system), b) ASHRAE (For Precision Air Conditioning). c) IS1893:1984 for seismic protection	Self Declaration from the bidder that the DC is in compliance all the 3 standards. Also the bidder's proposed Data Centres should be TIA942/Tier III Compliant and should have the following certifications: • ISO 9001:2015(or later) • ISO/IEC 20000:2011(or later) • ISO/IEC 27001:2013 (or later)" for which the bidder should furnish the Certified copy of Certificate issued by competent authority"
4	The bidder must have on its payrolls at least 100 technically qualified professionals (BE/B.Tech./MCA or equivalent) in the ICT domains i.e. Cyber security, networking, system software, systems integration, storage, etc. who have prior experience in providing the Data Center Infrastructure and maintenance services as on date of release of this RFP.	The bidder must have on its payrolls at least 50 technically qualified professionals (BE/B.Tech./MCA or equivalent) in the ICT domains i.e. Cyber security, networking, system software, systems integration, storage, etc. who have prior experience in providing the Data Center Infrastructure and maintenance services as on date of release of this RFP.
9	Bidder should have experience of Providing/ Managing Data center services of atleast 2 banks (public, private, scheduled commercial) in India in last 2 years	Self-Declaration certificate, with details offered to banks and relevant documents

3.31 Evaluation of Technical Bids

TECHNICAL SCORING			
Sr	**Description**	**Marks**	**Documents required**
	Credentials (A)	**30**	
2	**Financial Criteria**	5	
	The bidder's annual turnover from India Data Centre Services and Managed Services should be at least (INR) 100 crores in each of last three financial years (2015-16, 2016-17, 2017-18) and bidders company should be profitable in last 3 years. 2 marks to be deducted from scoring if the company is not profitable. >= (INR) 100 Crores < 125 Crores (2 Marks) >=(INR) 125 < 150 Crores (3 Marks) >=(INR) 150 Crores (5 Marks)		CA Certificate indicating turnover from Data Centre Services and Cloud & Managed Services from India operations

5.12 Tentative Bill of material

6.9.1 For DC

S.No	Items	Qty	For Commercial Reference
1	Physical firewall NGFW with UTM (IPS/IDS, AV Gateway, Sandboxing) External	2	OPEX
2	Physical firewall with IPS	2	OPEX
3	Core Switch 48 port	2	OPEX
4	Access Switch	2	OPEX
5	Bare metal Rack servers	20	CAPEX
6	SAN Switch	2	CAPEX
7	Storage SSD 50 TB Usable	1	CAPEX
8	Storage SATA 100TB Usable for backup and Logger	1	CAPEX
9	MS Windows Std per 2 core	105	CAPEX
10	RHEL 2 socket	1	CAPEX
11	Vmware Vsphere per socket	6	CAPEX
12	Vmware Vcenter	1	CAPEX
13	MS SQL Std per 2 core with SA*	12	CAPEX
14	MS SQL Ent per 2 core with SA*	33	CAPEX
15	Backup Software (30Tb Storage included in SATA Storage) and other required dedicated infra like media server etc.	1	OPEX
16	DRM solution with Dedicated infra	1	OPEX
17	SAP Crystal Report User based License	20	CAPEX
18	Replication Link P2P 10 Mbps	1	OPEX
19	Cross Connect of 100 Mbps	1	OPEX
20	Hosting	3	OPEX
21	Managed Services and Industry leaders Management tools as a service Solution	1	OPEX
22	HIPS Solution with required Dedicated Infra	For all servers Proposed	OPEX
23	IDAM with required Infra, can be virtualized on dedicated infra	100	OPEX
24	PIM with required Infra, can be virtualized on dedicated infra	18	OPEX
25	DAM with required Infra, can be virtualized on dedicated infra	8	OPEX
26	MFA with dedicated Solution in HA	100	OPEX
27	VA Service	20	OPEX
28	PT Service	10	OPEX
29	Hardware Load Balancer with WAF in HA	2	OPEX
30	DDOS 1Gbps Mitigation at ILL	1	OPEX
31	DDOS Dedicated Appliance	2	OPEX

*** SQl SA (Software Assurance) licenses can be used to reduce the no. of licenses required in DR but should comply to the licensing agreement with Microsoft.**

6.9.2 For DR:

S.No	Items	Qty	For Commercial Reference
1	Physical firewall NGFW with UTM (IPS/IDS, AV Gateway, Sandboxing) External	1	OPEX
2	Physical firewall with IPS	1	OPEX
3	Core Switch 48 port	1	OPEX
4	Access Switch	1	OPEX
5	Bare metal Rack servers	17	Capex
6	SAN Switch	1	Capex
7	Storage SSD 50 TB Usable	1	Capex
8	Storage SATA 100TB Usable for backup and Logger	1	Capex
9	MS Windows Std per 2 core	87	Capex
10	Vmware Vsphere per socket	2	Capex
11	Vmware Vcenter	1	Capex
12	SAP Crystal Report User based License	20	Capex
13	Backup Software (30Tb Storage included in SATA Storage) and other required dedicated infra like media server etc.	1	OPEX
14	Cross Connect of 100 Mbps	1	OPEX
15	Hosting	3	OPEX
16	Managed Services and Industry leaders Management tools as a service Solution	1	OPEX
17	Antivirus Solution With required Dedicated Infra	For all Servers Proposed for DC, DR and 1000 Users	OPEX
18	HIPS Solution with required Dedicated Infra	For all servers Proposed	OPEX
19	IDAM with required Infra, can be virtualized on dedicated infra	100	OPEX
20	PIM with required Infra, can be virtualized on dedicated infra	18	OPEX
21	DAM with required Infra, can be virtualized on dedicated infra	8	OPEX
22	MFA solution with required dedicated infra	100	OPEX
23	VA Service	6	OPEX
24	Hardware Load Balancer with WAF	1	OPEX
25	DDOS 1Gbps Mitigation at ILL	1	OPEX
26	DDOS Dedicated Appliance	1	OPEX
27	MS SQL Std per 2 core *	12	CAPEX
28	MS SQL Ent per 2 Core *	27	CAPEX

*** SQl SA (Software Assurance) licenses can be used to reduce the no. of licenses required in DR but should comply to the Microsoft licensing Policy.**

6.9.3 Near DR:

S.No	Items	Qty
1	Physical firewall	1
2	Bare metal Rack servers (12 Core)	1
3	MS Windows Std per 2 core	6
4	SAN Switch	1
5	Storage SSD 50 TB	1

Annexure D- Telecom Location

Telecom

S.NO.	Product	Branch Name	Branch / Location Address	Link 1 Band width	Link 2 Bandwidth
6	P2P	Point to Point link between proposed DC to Switch at Mumbai	BKC Data Centre, Tata Communications Ltd., IDC-1, 3rd. Floor, B Building, G Block, Bandra Kurla Complex, Bandra East, Mumbai 400053	To be Treated as deleted	
7	P2P	Point to Point link between proposed DR to Switch at Mumbai	BKC Data Centre, Tata Communications Ltd., IDC-1, 3rd. Floor, B Building, G Block, Bandra Kurla Complex, Bandra East, Mumbai 400053	To be Treated as deleted	
8	P2P	Point to Point link between proposed DC to Switch at Chennai	Tata Communications Ltd., 3rd. Floor, Videsh Sanchar Bhavan No.4, Swami Sivananda Salai, Chennai – 600002	To be Treated as deleted	
9	P2P	Point to Point link between proposed DR to Chennai	Tata Communications Ltd., 3rd. Floor, Videsh Sanchar Bhavan No.4, Swami Sivananda Salai, Chennai – 600002	To be Treated as deleted	
152	MPLS VPN	SOC Center - Noida	THE NAINITAL BANK LTD., Regional Office, Naini Business Centre, 4th Floor, UPRNN Building, C-20/1A/7, Sector 62, Noida – 201 309	To be Treated as deleted	
New	P2P	Point to Point link between proposed DC to proposed NDR		Bidder to propose on Fiber to achieve Zero Data Loss(RPO = Zero)	Bidder to propose on Fiber to achieve Zero Data Loss(RPO = Zero)
New	P2P	Point to Point link between proposed NDR to proposed DR		8 Mbps	8 Mbps
New	P2P	P2P Link from proposed DC to proposed SOC	Proposed Managed SOC Centre	4 Mbps	4 Mbps

6.18 Next generation firewall - Monitoring and Management

Few Activities to manage NGFW, but not limited to:

I. Traffic Profiling
II. Define Alert levels and Incident response level
III. Root cause analysis
IV. Technical support
V. Monitor NGFW for 24*7 availability
VI. Restore NGFW availability
VII. Determine Intrusion occurrence, zero day attack management, etc.
VIII. Upgrade of vendor provided signatures
IX. Provide security event correlation
X. Regular Monitoring of the attack logging rules' logs
XI. Regular Monitoring of the generic deny rules' logs
XII. Regular Monitoring of the attack bandwidth utilization
XIII. Network attacks and serious attack attempts analysis
XIV. Uncovered new vulnerabilities assessment
XV. Propose corrective and preventive actions.
XVI. Monitoring and subscribing to external network security information in order to evaluate new attacks and propose preventive s teps.
XVII. Regular Reports
XVIII. Incidence response
XIX. Prevent all known/zero day attacks
XX. Filter out IP and TCP illegal packet types
XXI. Design and Configuring IPS services in response to Flooding limits (per source, destination and intensity)

7. Annexure A : Hardware/Software Technical Compliance

7.1 Server Sizing

S.No	Components	Specifications	Qty DC	Qty in DR
1	Server Type 1	2x Intel® Xeon® Gold 6128 3.4G,6C/12T,10.4GT/s 2UPI,19.25M Cache,Turbo,HT (115W) DDR4-2666, 64 Gb RAM, 300GB 15K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive x 4, 2 Port SFP+ with multimode trans receivers and cables, Separate Management port, Dual Port 16Gb Fibre Channel HBA, RPS	4	4
2	Server Type 2	2x Intel® Xeon® Gold 6128 3.4G,6C/12T,10.4GT/s 2UPI,19.25M Cache,Turbo,HT (115W) DDR4-2666, 128 Gb RAM, 300GB 15K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive x 4, 900GB 15K RPM SAS Disk x 4, 2 Port SFP+ with multimode trans receivers and cables, Separate Management port, Dual Port 16Gb Fibre Channel HBA, RPS	6	6

3	Server Type 3	2x Intel® Xeon® Gold 6128 3.4G,6C/12T,10.4GT/s 2UPI,19.25M Cache,Turbo,HT (115W) DDR4-2666, 64 Gb RAM, 300GB 15K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive x 4, 2x 900 GB SAS 15K RPM disk, 2 Port SFP+ with multimode trans receivers and cables, Separate Management port, Dual Port 16Gb Fibre Channel HBA, RPS	2	2
4	Server Type 4	1x Intel® Xeon® Gold 6128 3.4G,6C/12T,10.4GT/s 2UPI,19.25M Cache,Turbo,HT (115W) DDR4-2666, 64 Gb RAM, 300GB 15K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive x 4, 2 Port SFP+ with multimode trans receivers and cables, Separate Management port, Dual Port 16Gb Fibre Channel HBA, RPS	4	4
5	Server Type 5	1x Intel® Xeon® Gold 6128 3.4G,6C/12T,10.4GT/s 2UPI,19.25M Cache,Turbo,HT (115W) DDR4-2666, 128 Gb RAM, 300GB 15K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive x 4, 4x 1.2TB SAS 15K RPM disk, 2 Port SFP+ with multimode trans receivers and cables, Separate Management port, Dual Port 16Gb Fibre Channel HBA, RPS	1	0
6	Server Type 6 (Log Server)	2x 3.0 GHz 6136/150W 12C/24.75MB Cache/DDR4 2666MHz, DDR4 128 Gb RAM, 4x 900GB 12G SAS 15K RPM SFF HDD, 2 Port SFP+ with 10G multimode trans receivers and cables, Separate Management port, Dual Port 16Gb Fibre Channel HBA, RPS	3	1
7	Other servers for management monitoring, AV, Security tools etc deployment	2x2.4 GHz 6148/150W 20C/27.50MB Cache/DDR4 2666MHz, DDR4 256 Gb RAM, 300GB 15K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive x 4, 2 Port SFP+ with multimode trans receivers and cables, Separate Management port, Dual Port 16Gb Fibre Channel HBA, RPS, Vmware License	As per solution	As per solution

7.5 Storage

Sr. No	Storage	Compliance (Yes/No)	Remarks/ Reference
1	OEM must be Leader in Gartner Magic Quadrant for Storage from last 3 years.		
2	The proposed storage system should be of Enterprise class All SSD/ Flash /FMD storage		
3	The storage should be able to scale to 100 TB capacity or higher using SSD/Flash Disks/FMDs of capacity less than 8TB		
4	The storage system must support intermixing of all SSD/FMD sizes in a same drive enclosure / chassis / shelf. The supported disks should be dual ported with minimum 6Gbps/12Gbps full-duplex data transfer capability		
5	Offered Storage Array shall be supplied with minimum of Two controllers & should be supporting all Block and File protocols for flexibility & ease of management		
7	The storage must provide non disruptive firmware/microcode upgrade, device reallocation and configuration changes		
8	The proposed storage system should support upto 4000 LUNs /Volumes or more		
9	The storage system should support Clusters of MS-SQL, My SQL,PostgreSQL, and Windows and Linux server clusters.		
10	The storage system should be configured with 64 GB Cache across HA with an ability to protect data on cache if there is a controller failure or power outage. The usable cache should only be used for reads & writes of workloads. The storage array must have complete cache protection using mechanism like mirroring/ de-staging/coherency SSDs will not be considered as cache memory.		
11	The storage array must have complete cache protection using mechanism like mirroring/ de-staging/coherency. Also provide complete cache data protection with battery backup for up to minimum 48 hours. The data shall not be lost in the case of power failure.		
12	Unified Storage solution should have block and file access with no Single Point of Failure, SPoF, and with host connectivity for FC, iSCSI, CIFS, NFS and FCoE. Storage should Scale more than 100 no. of Drives with dual controller system. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities.		

13	Should support various RAID levels (like Raid 5/6 or Equivalent)		
14	The Storage system should have Inline De-duplication & Inline compression feature for both file and Block bit type of data otherwise extra usable storage capacity needs to be factored as per below clause		
15	The storage should be supplied with rack mount kit.		
16	The storage system should be supplied with all the necessary SFP+ modules & patch cords as required		
17	Storage Solution Should be accommodated in a standard 42U 19" rack.		
18	The storage should be supplied with rack mount kit. The storage system should be supplied with all the necessary SFP+ modules & patch cords as required. Storage Solution Should be accommodated in a standard 42U 19" rack.		
19	The storage array shall have the ability to expand and contract LUNS/Volumes on the storage online and instantly. The Storage array must provide capability for thin provisioning of capacity. Vendor should provide the licenses for maximum supported capacity of the proposed storage		
20	The storage should have Quality of Service features for both file and Luns		
21	The proposed storage should have capability to do storage based IP replication with another storage at DR/DC. Replication should be storage based and integrated with storage system. Otherwise, the solution should include all the hardware like FC-IP routers, either built-in or supplied separately, if required to fulfil the replication solution.		
22	For maintaining Zero Data Loss in future, the required software capabilities should be included now and the hardware (ports, switches) required to achieve the same should be proposed now but will be procured later		
23	The solution shall support replication for the full supported capacity of the system and incenses should be provided for entire capacity		
24	The storage system should support remote replication for both file and block. After data is replicated at remote storage, data should be stored with "Data De-duplication and Compression". Any additional hardware or software required to achieve the same should be provided along with replication solution. For OEMs not supporting data deduplication, double capacity should be provided .		
25	The proposed storage system should have redundant hot swappable components like controllers, disks, power supplies, fans etc.The proposed storage must support non disruptive replacement of hardware component. Architecture shall support isolation of failed components automatically without rebooting/failing the entire storage.		
26	The solution shall support replication in one to many and many-to-one mode. The replication solution on storage shall support failover to BCP/DR storage and failback as and when required using DC, DR and NDR		
27	The array should support controller based functionality for pointer based snapshot. The storage should support minimum 250 snapshots per volume/LUN		
28	Vendor should provide the licenses for supported capacity of the proposed storage		
29	It should be possible to switch storage resources from storage system in one site to storage system in another site in case of any outage. All required hardware, software & licenses components required to provide the above functionality in the secondary site should be included as part of the proposal from day one.		
30	The system should support instant creation of clones of active data, with near zero performance impact for both block and file from lun/volume and existing snapshots. Necessary license to clone & restore from clone to be provided. Vendor should provide the licenses for maximum supported capacity of the proposed storage		
31	Easy to use Single GUI based and web enabled administration interface for configuration (Create, delete, configure Lun, Tiering Alerts , Cloud configuration and DR Replication) Friendly GUI Based Storage Administration tools for role based access control ,monitoring , even management and closure , threshold setting, LUN mapping , deallocation ,space reclaim etc. including management of DR and Near DR replication.		
32	GUI Based Storage Monitoring tools to obtain Storage performance statistics like Total IOPs performance , Read/write percentages, Store historical data , Management Dashboard etc		

33	The storage shall support logical/Virtual partitioning/multitenancy of controllers in future such that each partition appears as a separate storage in itself. Vendor should provide the storage virtualization licenses for maximum supported capacity of the proposed storage		
34	The proposed storage should support industry-leading Operating System platforms including: Suse and Red Hat LINUX, Microsoft Windows, HPUX, SUN Solaris, IBM-AIX, etc		
35	It shall support connecting hosts over iSCSI or FC and shall be supplied with any Multipathing/Equivalent software, if required, with the solution for unlimited host connectivity		
36	All the licenses on the storage system must be provided for maximum capacity supplied with the system from day one.		
37	Any hardware & software components required to enable the replication/DR solution will need to be provided, in requisite quantities of each, by the vendor		
38	The storage system must be supplied with Data-at rest encryption and key management solution (for Storage) The storage should be supplied with SSD 50TB(DC) and SSD 50TB (DR)usable capacity (Excluding any RAID overhead, Hot spare, Controller OS overhead, Snapshots and Clone overheads etc.) in dual disk failure protection with Data Deduplication and Compression enabled		
39	The designed IOPs for 30:70 Write: Read for the above systems for Raid 6 or equivalent should be minimum 1,00,000 The design document should be shared in the proposal		
40	The storage system should configured with 8 * 16 Gbps FC and 4* 10Gbe ports across dual controllers for iSCSI/NFS/CIFS. The system should have minimum 4x 12Gbps SAS backend ports.		
41	The Hardware and software quoted should have 5 years warranty and should have OEM support for 6 years from date of commissioning and acceptance, however it should not later than 2 weeks from delivery. 24X7 Support with 2 hrs response time for faults not requiring any spares, 4 hours response for faults requiring spares. All Licensing including 3 way Replication, Dedupe, compression, encryption etc. to be included		
42	Total downtime should not exceed 8 hrs in a year		

7.5.1 Log and Backup Storage

Sr. No	Storage	Features	Compliance (Yes/No)	Remarks /Refrences
1	Storage Quality Certification	The Storage OEM should be established in the Gartner Leader Quadrant for the last 3 years		
2	Storage Controller	The Storage system must have at least two controllers running in dual active (active-active) mode with automatic failover to each other in case if one controller fails		
3	Cache required	The system should have minimum 64 GB cache memory across the two controllers with an ability to protect data on cache if there is a controller failure or power outage. The cache on the storage should have 72hrs or more battery backup (OR) should have destaging capability to either flash/disk.		
4	Drive Support	The proposed system should not exceed the disk size of 8TB per disk and must support intermixing of SSD , SAS and SATA drives to meet the capacity and performance requirements of the applications.		
5	Protocols	The storage should be configured with FCP & iSCSI protocols. Any hardware/software required for this functionality shall be supplied along with it in No Single Point Of Failure mode.		
6	RAID configuration	Should support various RAID levels (1,5,6) or equivalent		
7	Storage Capacity	100 TB usable capacity should be configured with SATA HDD. The usable capacity is defined as the Net storage capacity available after deducting the penalties imposed by storage infrastructure requirements, disk and array formatting, RAID penalties etc.		
8	Drive Support	The system must support intermixing of SSD , SAS and SATA drives to meet the capacity and performance requirements of the applications. The system must support a minimum of a 180 disks per two controllers for scalability purpose.		

9	Front-End and Backend connectivity	The proposed storage system should have minimum, 2 numbers of 12 Gbps backend SAS ports, and 8 x 16Gbps FC and 4x10Gb Ethernet Ports		
10	Rack Mountable	The storage should be supplied with rack mount kit. All the necessary patch cords (Ethernet and Fiber) shall be provided and installed by the vendor.		
11	Storage functionality	The storage shall have the ability to expand LUNS/Volumes on the storage online and instantly.		
		The storage shall have the ability to create logical volumes without physical capacity being available or in other words system should allow over-provisioning of the capacity. The license required for the same shall be supplied for the maximum supported capacity of the offered storage model.		
		The required number hard disks for parity & spares, should be provided exclusively of the usable capacity mentioned. At least 2% of the usable capacity requested on each tier should be configured as spare drives with the subsequent disk types		
		System should have redundant hot swappable components like controllers, disks, power supplies, fans etc.		
12	Point-in-times images	The storage should have the requisite licenses to create point-in-time snapshots. The storage should support minimum 512 snapshots per dual controller system. The license proposed should be for the complete supported capacity of the system.		
		The system should support instant creation of clones of active data		
13	Management	Easy to use Single GUI based and web enabled administration interface for configuration, storage management, performance analysis tools and replication management		
14	OS support	Support for industry-leading Operating System platforms including: LINUX , Microsoft Windows, HP-UX, SUN Solaris, IBM-AIX, etc.It shall support connecting hosts over iSCSI or FC and shall be supplied with any Multipathing software, if required, with the solution.		
15	Warranty & SLA	The Hardware and software quoted should have 5 years support along with upgrade and updates.		

7.6 SAN switch

S No.	Specifications	Compliance (yes/NO)	Remarks
1	Make & Model of the proposed San switches		
2	Part Code of the proposed San Switches		
3	The SAN Switch should be Fibre Channel based SAN Switch should be of 24 ports with 16 Gbps speed.		
4	Switch SFP's should support the 2/4/8/16 Gbps of host connection.		
5	Per switch connectivity required is as below : 16-Gbps SFP (supporting 4/8/16 Gbps Speed) - 48 qty		
6	Should support incremental activation of ports on demand		
7	Should support the following minimum type of ports: E_Port, F_Port, M_Port (Mirror Port), NPIV-enabled N Port		
8	The form factor should not be greater than 1RU		
9	Should support the following minimum media types: SFP+, LC Connector and multiple variants industry standard connectors. Switch & optics must be from same OEM.		
10	The SAN Switch solution with redundant switches should be highly available with no single point of failure		
11	Switch should support non-disruptive code/Firmware upgrade		
12	The switch should support role based administration by allowing different administrator different access rights to Switches		
13	Should have Hot Plug Redundant Power Supplies and cooling fans		
14	Should have Auto Sensing of ports		

15	Must support heterogeneous hosts and operating systems		
16	Must have Advance Zoning feature		
17	The offered SAN Switch must support leading SAN boxes, SAN Switches and Tape libraries including but not limited to EMC, Hitachi, IBM, HP, Dell, Cisco etc.		
18	Should have centralized monitoring and control features.		
19	The Product shall support any combination of Shortwave, Long wave optical media on a single switch.		
20	The vendor has to supply all necessary. Components / parts / license to meet the requirements at no extra cost to the Bank		
21	The SAN Switch should have capability to interface with HBA of different makes and model from multiple OEM, supporting multiple operating systems including but not limited to HP-UX, IBM AIX,Red Hat Linux MS-Windows Solaris etc		
22	Should support the Inter switch link (ISL) & necessary licenses need to be provision as a part of scope.		
23	Integration: Integration to be adequately done with existing SAN switch / SAN Storage / Backup Server / blades.		

7.7 Tape Library – Removed from Scope

7.9 Backup Tool

Page No	Sr. no	Specification as per original RFP Document	Amendment
92	16	Proposed solution should be licensed in processor or capacity based	Solution should be licensed on Processor/Capacity/Server/agent
91	3	Existing Clause states: Proposed solution should support Central web based Management Console that simplifies the process of managing and reporting on multiple backup servers & Desktops in distributed across an environment.	Backup Software must support GUI with centralized management / Single interface for management of all backup and archival (file system and E-mail) activities across physical servers, VMs. Branches and end point backup is not in scope
92	12	The proposed backup solution should support online backup solutions for different types of databases such as Oracle, MS SQL, Sybase, SQL etc. on various OS. A combination of backup solution is acceptable	Backup software should be able to protect the following through online agents enabling granular restores. Major DBs like Oracle, Exchange, Sybase, Informix, DB2, MS SQL, MySQL, MongoDB, MariaDB, etc. and Applications likes SAP, etc. across wide range of popular Windows / Linux and Unix flavours.
91	3	Existing Clause states: Proposed solution should support Central web based Management Console that simplifies the process of managing and reporting on multiple backup servers & Desktops in distributed across an environment.	Backup Software must support GUI with centralized management / Single interface for management of all backup and archival (file system and E-mail) activities across physical servers, VMs. Branches and end point backup is not in scope
92	18	The software should be able to use USB drives/Network file share/block storage / and native file server volumes for keeping the backup copies	The software should be able to use Network file share/block storage and native file server volumes for keeping the backup copies
	30	Backup software Must be present as Leaders in Gartner's Magic Quadrant for backup software for last 3 years	New Point
	31	Offered solution should have the ability of detecting Ransomware malware on client computer. Any attempt to backup ransomware affected data should be flagged off by a notification to the administrator. Solution should have the ability to configure automated tasks like removing the computer from the network and send notification mails.	New Point
	32	Backup software should have the ability to archive data and create a single repository for backup and archive for space efficiency and easier data management.	New Point

	33	Backup software should be able to replicate backed up data in de-duplicated format (for bandwidth optimization) to another site for compliance purposes, with or without the need of external replication tools. All necessary hardware and licenses for achieving consistent replication of backup data should be quoted.	New Point
	34	It should support the following algorithms and provide better security in deployment across sites - BLOWFISH, GOST, Serpent, AES, Twofish, 3-DES, etc.	New Point

7.10 Annexure B: Cyber Security Technical and Functional Compliance

All OEM should be in leaders/Challenger Gartner quadrant in networking, security and application delivery controller

7.10.1 NGFW (Firewall+IPS+URL+ zero dat + Anti-virus/Anti-Bot)

The entire table in RFP to be replaced with this table

S.No	Specification	Specification proposed by bidder	Compliance (Y/N)
1	Fixed architecture		
2	Solution should be appliance based multi-core Processing Technology		
3	Minimum storage minimum 100GB SSD		
4	Dual Power supply		
5	Minimum 2 x 10G SFP+ Interfaces. All ports should be populated with 10G multimode transceivers		
6	Minimum 8 x 10/100/1000 copper Interfaces		
7	Solution shall provide features of Firewall, IPS, URL filtering, Anti-Bot, Anti Malware & Zero-day Threat Protection, VPN and Application Control on same platform		
8	Threat Prevention throughput should be 5 Gbps measured on Mix Traffic		
9	Minimum IPsec VPN throughput – 10 Gbps		
10	Minimum tunnels (SSL, IPSec) – 200		
11	Concurrent Sessions – 100, 00,000		
12	Connections/Sessions per sec – 2,000,00		
13	Active/Active, Active/Passive		
14	The proposed firewall shall support network traffic classification which identifies applications across all ports irrespective of port/protocol		
15	The proposed firewall shall be able to create custom application signatures and categories		
16	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Service and threat protection profile under the same firewall rule or under different set of polices		
17	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application base on the content.		
18	Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.		

19	Should block know n network and application- layer vulnerability exploits		
20	The proposed firewall shall perform content based signature matching beyond the traditional hash base signatures		
21	The proposed firewall shall have on box Anti- Virus/Malw are, Anti Spyware signatures and should have minimum signatures update w indow of 600 seconds.		
22	All the protection signatures should be created by vendor base on their threat intelligence		
23	Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firew all policy to block those malicious attributes and list should get updated dynamically w ith latest data		
24	This should be a cloud base unknow n malw are analysis service w ith guaranteed protection signature delivery		
25	Advance unknow n malw are analysis engine should be capable of machine learning w ith static analysis and dynamic analysis engine		
26	appliance based unknow n malw are analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection w hich is uploaded to unknow n threat emulation and analysis		
27	on premise malw are analysis appliance should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Web pages that include high-risk embedded content like JavaScript, Adobe Flash files		
28	The proposed next generation security platform should be able to detect and prevent zero day threats		
29	Same Hardw are platform should be scalable to provide URL filtering and w eb protection and should maintain same performance/throughputs mention in primary scope		
30	The proposed firewall shall have the database located locally on the device or in the attached management server / appliance		
31	The proposed firewall shall support custom URL-categorization		
32	The proposed firewall shall support customizable block pages		
33	The proposed firewall shall support logs populated w ith end user activity reports for site monitoring (locally or via separate management solution)		
34	The proposed firewall shall support URL Filtering policies by AD user, group and IP address/range		
35	Should support full-path categorization of URLs only to block the malicious malw are path not the full domain or w ebsite		
36	Should support zero-day malicious w eb site or URL blocking update for URL DB update for zero-day malw are command and control, spyw are and phishing w ebsites access protection		
37	Should support URL or URL category base protection for user cooperate credential submission protection from phishing attack w ith malicious URL path		
38	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection		
39	The proposed firewall must support the follow ing routing protocols:		
	Static		
	OSPFv2 and v3 w ith graceful restart		
	BGP v4 w ith graceful restart		
	Policy-based forwarding		

	PIM-SM		
40	Should support the following authentication protocols:		
	- LDAP		
	- Radius		
41	The proposed firewall's SSL VPN shall support the following authentication protocols		
	- LDAP		
	- Radius		
	- Any combination of the above		
42	Should support on device or centralized management with complete feature parity on firewall administration		
43	Should have separate real time logging base on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities		
44	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis		
45	Should allow the report to be exported into other format such as PDF, HTML etc.		
46	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs		
47	There shall be provision for logging, reporting, management etc. either through on-device arrangement or through external management server on premise.		
48	The device or management server shall be able to keep logs for minimum 1 year or store logs up to 1TB.		

8 Internal Firewall

S.No	Specification as per original RFP Document	Amendment
22	Should protect against DoS / DDoS / SYN- flood/ TCP-flood/UDP-flood	Point to be considered removed
23	Must have "Zero-day" protection against DoS / DDoS and worm attacks based on traffic behaviour.	Point to be considered removed

11 Endpoint security

S.No	Specification as per original RFP Document	Amendment
26	Configure Web reputation policies and assign them to individual, several, or all endures machine.	Point to be considered removed
62	Centralized management server should be able to automatically report about the new unprotected endpoints in IOCL network"	Centralized management server should be able to automatically report about the new unprotected endpoints

12 AAA

S.No	Specification as per original RFP Document	Amendment
11	The AAA server should support LDAP Configuration Interface(LCI) to allow scripting	Point to be considered removed
12	The AAA server should support directed realms to provide virtualized instances of the server, allowing requests to be managed according to their nature	The AAA server should support virtualized instances of the server, allowing requests to be managed according to their nature.
15	The AAA server should support Proxy filtering	Point to be considered removed

13 IDAM (IAM duplication removed)

S. No.	Minimum Specification	Specification proposed by bidder	Compliance (Y/N)
1	Proposed solution should collect identity, entitlement, and role information from various information resources across the enterprise. The solution should have the following collection capabilities:		
2	The solution uses agent-less connections		
3	The solution needs to be able to collect information such as: accounts, identity, roles & entitlements)		
4	The solution should be able to normalize and aggregate identity and entitlement information to provide a composite view of user access (Specifically explain supporting multiple sources of identity)		
5	The solution should support collection from, but not limited to, the following target system like		
6	Google Apps		
7	Amazon AWS		
8	Sharepoint		
9	Active Directory		
10	Office365		
11	Oracle, DB2, MySQL, Sysbase, MS SQL		
12	The solution should provide a way to designate accounts as privileged or system accounts from the User Interface.		
13	The solution should detect and alert administrators to newly discovered orphaned accounts from an entitlement source (i.e.: accounts that are not associated with any known user)		
14	The solution should provide a clear indication of compliance violations during the certification process.		
15	The solution should enable certification based on a specific set of users or groups?		
16	The solution should enable certification based on an application or role owner.		
17	The solution should automatically generate certifications based on detected changes to a user's relationship to the organization (e.g., user changes department or is terminated)		
18	Solution MUST be pre-packaged without the need for development and should be provided with necessary Operating System in high availability mode and along with the necessary SSL certificate.		
19	Solution MUST be physical or virtual as per bidder solution		
20	Solution MUST be able to perform SSO for Unix (client/server) without additional development or cost.		
21	Solution MUST be able to perform SSO for any firewall without additional development or cost.		
22	Solution MUST be able to perform SSO for all the application without any additional development		
23	Solution MUST support a PRE-Windows logon self-service password resets.		
24	Solution MUST operate even with the loss of connectivity to the central repository		

25	Solution MUST be able to authenticate against multiple LDAP directories in a multi-domain Active Directory forest.		
26	Solution MUST have redundancy and failover capabilities built in.		
27	Solution MUST support multiple challenge response questions to authenticate a user before allowing self-service password reset		
28	Solution MUST support user self-service for password resets		
29	Solution MUST support multiple password policies.		
30	Solution MUST service forgotten and/or expired passwords		
31	Solution MUST support basic HTTP authentication		
32	Solution MUST support FORMS based authentication		
33	Solution MUST provide transaction level audit/reporting on access to protected resources.		
34	Solution MUST support advanced authentication such as digital certificates, tokens and multiple factor, swipe cards.		
35	Solution MUST have a shared workstation solution for single sign-on.		
36	Solution MUST have no JRE dependencies		
37	Solution MUST use LDAP directory credentials as the primary account.		
38	Solution should support the ability for solution administrators to manage roles.		
39	Solution should limit attribute displays from queries according to access/privacy policies.		
40	Solution should support strong password (i.e. 8 character with special, alpha, numeric, case, non-repeat, short expiration)		
41	Solution should support logout from application, portal or domain if the user is idle		
42	Solution should support timeout policy from application, portal or domain.		
43	Solution should support encrypted network communications between components and end points		
44	Solution should support failover and recovery from failure of any part of the system		
45	Solution should support integration with existing VPN technologies		
46	Solution should support scalability.		
47	Solution should support ODBC compliant third party reporting tools.		

14 PIM – The entire table for PIM should be replaced with the table given under

S. No.	Minimum Specification	Specification proposed by bidder	Compliance (Y/N)
1	Solution should support multiple and tightly couple security layers - Encryption, Access Control, Authentication		
2	Support for High Availability & Disaster Recovery		
3	Architecture design needs to ensure complete separation of data between customers in the Vault with logical containers.		
4	Solution should be TLS 1.2 and SHA-2 compliant for PCI-DSS compliance		
5	Solution should support agentless web based & light weight architecture		
6	Should support high availability and disaster recovery		
7	Console allows many to many grouping for enforcing policy based restriction to specific users or group of users		
8	Should support for multiple browsers like Chrome, Firefox, Internet Explorer		
9	Password age is managed based on password change date		
10	Enable secure password storage of privileged identities without human intervention.		
11	100% Active Directory & LDAP Integration		
12	Dual Factor Authentication using Biometric Devices, Hardware Token & Mobile based OTP		
13	Maker-checker approval for critical PIM configuration activities		
14	Support for transfer of files using SFTP over SSH		
15	Integration with Third party SIEM solution		
16	Configuration Command profiles allows administrators to configuration access permissions on UNIX / databases / windows at group / user level.		
17	Enhanced Segregation of Duties within PIM solution		
18	User profile based console level restriction on Windows Platform		

19	S.M.A.R.T. Audit Trails for user activity tracking		
20	Dashboard should provide real-time view of activities performed by users		
21	Users can be notified via email / SMS for any changes to PIM configuration, administration and user activity		

17 DDOS

Slno	Technical Specifications	Compliance (Yes/No)	Remarks
1	DDoS Detection & Mitigation solution being offered should be minimum EAL 2 certified or higher. OEM must be present in the latest Forrester "LEADER" Quadrant for DDoS technology. DDoS Mitigation solution vendor should have OEM TAC in India.		
2	DDoS mitigation solution should be a dedicated appliance (not a part of Router or Application Delivery Controller or Proxy based architecture or StateFul Device).		
3	Dedicated appliance based DDOS Mitigation solution (not a part of Firewall or Router or ADC or Proxy based Architecture) with DoS Flood Attack Prevention Rate: upto 25 Mpps (EAL 2 or above certified) Inpsection Ports supported : Minimum 8 x 10G SFP+ and 8x 1G copper		
4	DDoS Mitigation device should support throughput capacity of 4 Gbps from day 1 and scalable upto 10 Gbps with additional license (without changing the Hardware)		
	Security Protections:		
5	BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against threats, including Mirai DNS Water Torture, Burst and Randomized attacks.		
6	POSITIVE SECURITY MODEL should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic		
7	ZERO DAY ATTACK PROTECTION should be provided by behavior-based protection with automatic signature creation against within few seconds of unknown, zero-day DDoS attacks.		
8	CUSTOM TAILORED HARDWARE must be proposed using dedicated DoS Mitigation platform which off-loads high volume attacks, inspecting without impacting user experience.		
	Behavioural DoS Protection		
9	Behavioural DoS (Behavioural Denial of Service) Protection should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Device should support automatic Real Time Signature creation. Network-flood protection should include: • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood		

	• UDP flood • ICMP flood • IGMP flood		
	Security Features – Signature Protections support		
10	• Server-based vulnerabilities: — Web vulnerabilities — Mail server vulnerabilities — FTP server vulnerabilities — SQL server vulnerabilities — DNS server vulnerabilities — SIP server vulnerabilities • Worms and viruses • Trojans and backdoors • Client-side vulnerabilities • IRC bots • Spyware • Phishing • Anonymizers		
	EMERGENCY RESPONSE TEAM service required from DAY1		
11	The OEM has to provision for knowledgeable and specialized security experts who provide 24x7 (SLA defined), REAL TIME Professional Services for the network facing denial-of-service (DoS) attack in order to restore network and service operational status. The service should NOT be a part of TAC support or SoC Team support, rather it should be a OEM Professional Services team which would be taking care for the DoS/DDoS Flood Mitigation services on real time basis.		
12	The ERT should support the following advanced services: 1) 24/7 monitoring of the customer's service 2) Real-time response to any threat detected 3) Direct "hot-line" access 4) Diverting the traffic when encountering a volumetric attack 5) Sending the customer a summary of each real-time attack case 6) Sending the customer a monthly report containing all threats		

	7) Periodically reviewing the network-security configuration		
13	Centralized Monitoring and Reporting solution should be provided from Day 1		
14	The proposed solution should be able to Integrate with OEM Cloud based Scrubbing Centres, in case of Bandwidth Saturation attacks, using the same technology OEM.		
15	Centralized management and historical reporting solution to be provided from day 1.		

18 VAPT

S.No	Specification as per original RFP Document	Amendment
5	Bidder shall be responsible for VAPT Audit -4- VA and -2- PT in a year	New Point

19 MFA

S. No.	Specification as per original RFP Document	Amendment
1	Service should be available in subscription model	Consider the point to be Deleted

Other Amendments

Page No	Section	Specification as per original RFP Document	Amendment
51	5.4 Detailed Scope of Work -Telecom Scope of Work – Last Mile Link	Wireline Copper/Fibre – Atleast 50% of existing links. Request to consider 35% of links	Wireline Copper/Fibre – Atleast 60% of existing location should have primary link on Fiber/copper
51	5.4 Detailed Scope of Work -Telecom Scope of Work – Last Mile Link	VSAT links should not be more than 10% of total link.	VSAT links should not be more than 10% of total location.
51	5.4 Detailed Scope of Work -Telecom Scope of Work – Last Mile Link	Installation of 3G/4G at some locations as backup link under exceptional circumstances where roof top permissions are not available for RF/VSAT delivery	Installation of 3G/4G at some locations as backup link under exceptional circumstances where roof top permissions are not available for RF/VSAT delivery . Unmanaged service can be provided for link delivered on 3G/4G (If any)
52	5.4 Detailed Scope of Work -Telecom Scope of Work – CPE Devices	New point added as (i)	The SDWAN centralised controller should be hosted within India, in HA mode and should be in different geo-seismic zones
6	5.4 Detailed Scope of Work 4.74.7. Service Level Agreements	The selected bidder shall ensure an uptime more than 99.50% on a monthly basis for period of five years Its 99.90% for DC\DR and 98% for links.	Accepted: It should be 99.9% All Across Except the NON IT Component of Data center. Non IT Components of Hosted DC should be 99.5%
24	Solution Strength point 4	Service offering for Management, Analytics, Patch Management, Antivirus, Backup Software	Service offering for Management, Patch Management, Antivirus, Backup Software

20 Section IV: Financial Bid Format (Revised)

The Nainital Bank Limited
Summary : Supply, installation, testing and commissioning (SITC) of ICT infrastructure

(Price in Rs.)

S.No	Description	Total Price (excluding GST)	GST	Total Price (Including GST)
1	BOQ- DC-DR- **Table A** (Capex)			
2	BOQ- DC-DR-**Table B**(Opex)(cost for -5- yrs)			
3	BOQ – NDR **Table C**(Capex)			
4	Telecom (One Time Cost)			
5	Telecom (Opex) (cost for -5- yrs)			
	Total Contract Value (All Inclusive)			

Total contract value (Excluding GST/Other taxes) **of all OPEX** should be further divided by the number of bank's branch/offices on per month basis. (Billing will be monthly)

Total OPEX contract value (Excluding GST) - 60 Months (a)	Total OPEX / Month (b=a/60)	Total OPEX /Site/Month (c=b/145) – SLAB1 (up to 150 sites)	Applicable discount (in percentage) for all sites when no. of branches/Offices increases from 151 to 175 Sites	Applicable discount (in percentage) for all sites when no. of branches/Offices increases from 176 to 200 Sites

Terms & conditions:

1. The Bid Value shall be inclusive of all the installation, commissioning, testing and any other price that might be incurred by the Bidder for the performance of the contract

2. Bid will be evaluated on Total Contract Value(i.e. for -5- yrs) excluding Taxes. However GST shall be levied as per actuals as the time of invoicing.
3. CAPEX & OPEX ratio shall be reasonable and realistic, a bid may not be considered for Final Evaluation if the total CAPEX Value happens to be more than 60% of the overall bid value
4. All NDR Components mentioned in BOQ Above will be part of Capex Table C
5. Tape Library is removed.
6. Backup solution modified to disk based as per above BOQ. (Table B). It should be part of OPEX.
7. Other qty Change in BOQ as per the BOQ mentioned above.
8. Annexure D will be as per the updated Telecom BOQ above.

Revised Table A, B & C

The Nainital Bank Limited

CAPEX - Supply, installation, testing and commissioning (SITC) of ICT infrastructure

Table A -BOQ-DC-DR(Capex) (Price in Rs.)

S.No	Description	Qty-DC (a)	Qty-DR (b)	Basic Unit rate (c)	Total Price (excluding GST) (d)= (a+b)*(c)	Total GST (e)	Total Price (Including GST) (f)=(d)+(e)
1	Bare metal Rack servers	20	17				
2	SAN Switch	2	1				
3	Storage SSD 50Tb usable	1	1				
4	Storage SATA 100 Tb usable for Backup and Logger	1	1				
5	MS Windows Std per 2 core	105	87				
6	RHEL 2 socket	1	0				
7	VMware VSphere per socket	6	2				
8	VMware Vcenter	1	1				
9	MS SQL Std per 2 core with SA	12	0				
10	MS SQL Ent per 2 core with SA	33	0				
11	SAP Crystal Report User based License	20	20				
	Total - (Table A)						

Nainital Bank Limited
Supply, installation, testing and commissioning (SITC) of ICT infrastructure

(Price in Rs.)

Table B - BOQ-DC,DR and NDR (opex)

				Year 1		Year 2		Year 3		Year 4		Year 5			
S.No	Description	Qty-DC (a)	Qty-DR (b)	Basic Unit rate (c)	Total Price (excluding GST) (d)= (a+b)* (c)	Basic Unit rate (e)	Total Price (excluding GST) (f)= (a+b)* (e)	Basic Unit rate (g)	Total Price (excluding GST) (h)= (a+b)* (g)	Basic Unit rate (i)	Total Price (excluding GST) (j)= (a+b)* (i)	Basic Unit rate (k)	Total Price (excluding GST) (l)= (a+b)* (k)	**Total GST (m)**	**Total Price (Inclusive taxes) (n)=(d)+(f)+(h)+(j)+(l)+ (m)**
1	Physical firewall NGFW with UTM (AV Gateway, Sandboxing) External	2	1												
2	Physical firewall	2	1												
3	Core Switch 48 port	2	1												
4	Access Switch 24 Port	2	1												
5	Backup software (30 Tb storage included in SATA storage) and other required dedicated Infra like Media , Server etc	1	1												
6	DRM solution with infra	1	0												

7	Antivirus with required infra	0	For all Servers Proposed for DC, DR and 1000 Users												
8	Replication Link P2P 10 mbps	1	0												
9	Cross Connect of 100 Mbps	1	1												
10	Hosting rack space Including power, cooling and Physical security	3	3												
11	Managed Services and Industry leaders Management tools as a service Solution	1	1												
12	HIPS Solution with required Infra	For all servers Propose d	For all servers Proposed												
13	IDAM with required Infra, can be virtualized on dedicated infra	100	100												
14	PIM with required Infra, can be virtualized on	18	18												

	dedicated infra														
15	DAM with required Infra, can be virtualized on dedicated infra	8	8												
16	AAA With required Infra, can be virtualized on dedicated infra	2	1												
17	MFA With required Infra, can be virtualized on dedicated infra	100	100												
18	VA Service	20	6												
19	PT Service	10	0												
20	Hardware Load Balancer with WAF(HA in DC)	2	1												
21	DDOS 1Gbps mitigation at ILL	1	1												
22	DDOS dedicated appliance	1	1												
	Total - (Table B)														

Table C - BOQ - NDR(Capex) (Price in Rs.)

S.No	Description	Qty-NDR (a)	Basic Unit rate (b)	Total Price (excluding GST) (c)= (a)* (b)	Total GST (d)	Total Price (Including GST) (e)=(d)+(c)
1	Bare metal Rack Server- 12 Core	1				
2	MS Windows Std per 2 core	6				
3	Physical Firewall	1				
4	San Switch	1				
5	Storage SSD 50 Tb	1				
	Total - (Table C)					

----------END OF Document ----------